18.704 Fall 2004 Homework 7

All references are to the textbook "Rational Points on Elliptic Curves" by Silverman and Tate, Springer Verlag, 1992. Problems marked **(*)** are more challenging exercises that are optional but not required.

1. Do Exercise 3.9(a) from the text.

2. This problem is again about the curve $C : y^2 = x^3 + 3x$. Even if we have found the rank of an elliptic curve (as we have for this one in problem 1), it can be hard to find generators for the group of rational points. In this problem, I ask you to find generators for $\Gamma = C(\mathbb{Q})$. Any way you come up with for doing this is fine. The following steps outline one possible way, which you can ignore if you find a different way.

(a) By inspection, one can easily find the integer point $(1, 2)$ on C. Find all of the points on C with integer coordinates (Hint: Besides $(0, 0)$ and $(1, 2)$, I found two other integer points with positive y-coordinate, and I believe these are all of them. Note that an integer point $(x, y) \in C$ of infinite order need not satisfy the conclusion of the Nagell-Lutz theorem.)

(b)(*) Can you prove these are all of the integer points? (Since we have no theorems so far to help us find all integer points on a cubic, you'll have to invent some ad-hoc argument. I wasn't able to do it.) If you can't or choose not to solve part (b), just assume that you have all of the integer points and go on to (c).

(c) Show that if a rational point $Q = (x, y) \in C(\mathbb{Q})$ does not have integer coordinates, then mQ does not have integer coordinates for all $m \geq 1$ (Hint: review section II.4.)

(d) Prove that the set of points $\{P = (1, 2), T = (0, 0)\}$ generates the group Γ (assuming part (b) is true.) Remember this means that every element of Γ has the form $mP + nT$ for some $m, n \in \mathbb{Z}$.

3. Consider the curve $C : y^2 = x^3 + px$ for some prime $p \geq 2$ with group of rational points $\Gamma = C(\mathbb{Q})$.

(a) Do Exercise 3.8(a) from the text.

(b) If $p = 73$, show that the rank of Γ is 2.

4. Let C be the singular cubic curve $y^2 = x^3$. We have seen that if $\Gamma_{ns} = C(\mathbb{Q}) \setminus \{(0,0)\}$ is defined to be the set of rational points on C excluding the singular point $(0,0)$, then Γ_{ns} is a group (with identity point $[0,1,0]$ at infinity as usual, and the group law defined in the same way as for nonsingular curves.) In the following steps we will prove part (b) of the Theorem on page 100.

(a) Do Exercise 3.10(a) from the text. The formulas given in this problem do not work for all possible choices of points P, Q; what are the exceptions?

(b) Do Exercise 3.11 from the text. Note that the formula given there needs a minor correction, and that the exceptions to the formula of part (a) need to be dealt with.

(c) So Exercise 3.13(a) from the text. (Hint: it is enough to prove that given any finite set of rational numbers $q_1, q_2, \ldots q_m$, the set

$$\{a_1q_1 + a_2q_2 + \cdots + a_mq_m | a_1, a_2, \ldots, a_m \in \mathbb{Z}\}$$

is not all of $\mathbb{Q}$).